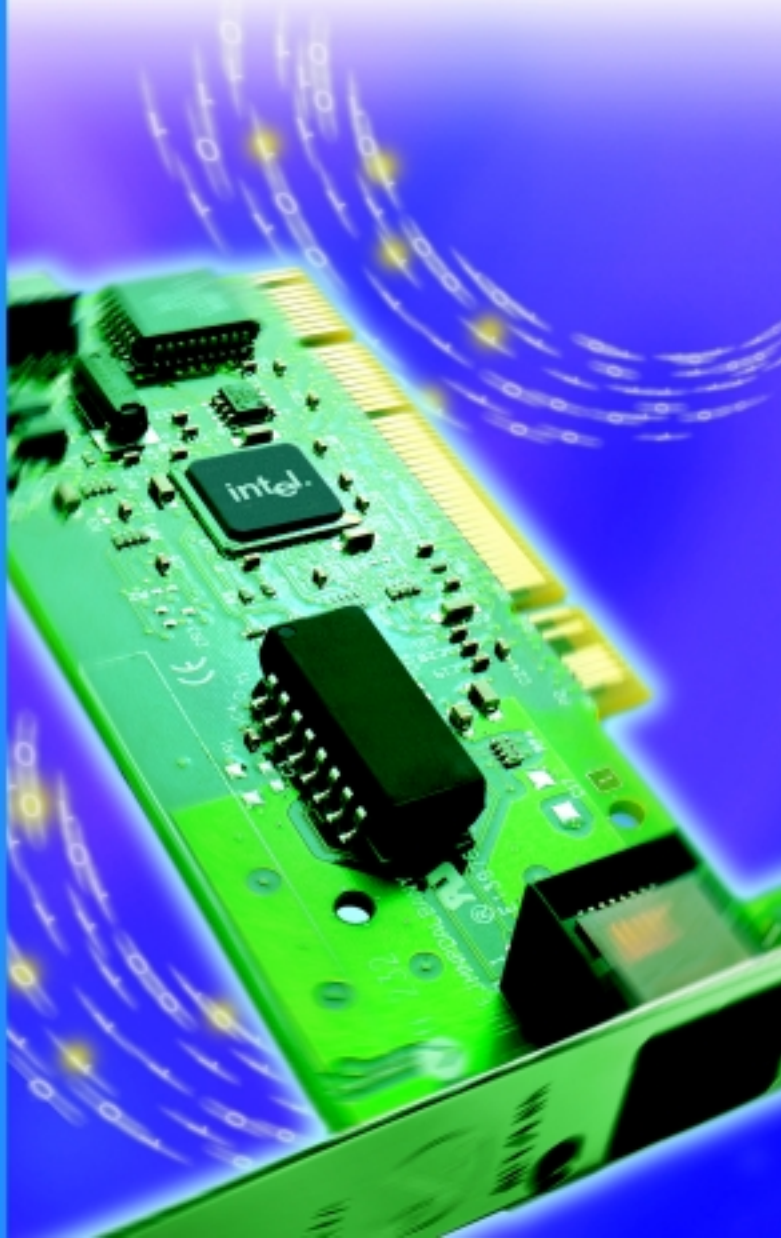


Intel® PRO/100 Family Packet Protect

*Enabling the IPSec Protocol on
Microsoft Windows NT® 4.0*

User's Guide



intel®

Where to Go for More Information

Readme Files

For more information about installation and general information about the product, see the readme text file. To view the files, view the root folder on the Intel CD-ROM. Open readme.txt with any text editor.

Online Services

You can use the Internet to download software updates, and to view troubleshooting tips, installation notes, and more. Online services are on the World Wide Web at:

<http://support.intel.com>

Copyright © 2000, Intel Corporation. All rights reserved.

Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, OR 97124-6497

Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

* Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Contents

Where to Go for More Information	ii
Contents	iii
Introduction	1
What is Intel® Packet Protect?	2
Packet Protect Features 2	
Complete Your Security Solution 2	
Hardware Acceleration 2	
Domestic and Export Versions 2	
Additional Information 3	
How Packet Protect Works	4
What is IP Security? 4	
What is Internet Key Exchange? 4	
The Process 5	
Get Started	6
Installing Packet Protect	7
Developing Your Deployment Model	8
Review Your Network Architecture and	
Corporate Security Guidelines	8
Assign security behavior roles to computers that you want to use	
Packet Protect 9	
Develop a strategy for handling pre-shared keys 10	
Understand the Default Rule 11	
Consider exceptions to the Default Rule 11	
What are the Trade-offs? 12	
Conclusion 14	
Set Up Intel Adapters	15
Install Intel Adapters 15	
Configure Intel Adapters 15	
Install Packet Protect	17
System Requirements 17	
Licensing 17	
Install Packet Protect 17	
View Your Security Settings	19

Configuring Security Settings	21
Understand Default Security Behavior	22
Default Behaviors in Packet Protect	22
Set up Your System Policy	25
What is a Policy?	25
What is a Rule?	25
The Default Rule	26
Importance of Rule Order	27
How Does the System Policy Work?	28
Add Rules to the System Policy	28
 Making Changes	 39
Modify the System Policy	40
Modify Destination Workgroups or Security Actions	41
Delete a Rule	41
Restore the System Policy	42
Monitor Packet Protect Computers	44
View Status at a Packet Protect Client	44
Set Up Compatible Policies	45
Work with Other Security Products	46
Turn Security On for a Computer	47
Install Security for a New Computer	47
Turn Security on Manually for an Existing Computer	47
Turn Security Off for a Computer	48
Shut Down Packet Protect at a Computer	48
Uninstall Packet Protect from a Computer	48
 Troubleshooting and FAQs	 49
Troubleshooting	50
Frequently Asked Questions (FAQs)	52
Appendix A — IKE and IPSec	53
.....	53
IKE and IPSec Work Together	54
How Packet Protect Uses IKE	55
Identity Negotiation Settings	55
IPSec Settings	57

Examples	58
How Packet Protect Uses IPSec	59
Security Associations	59
Security Association Lifetimes	59
How IPSec Protects Packets	60
Appendix B — Interoperability with Microsoft Windows* 2000	63
Interoperability with Windows* 2000	64
Appendix C — Network Software License Agreement	65
Network Software License Agreement	66
Intel Automated Customer Support	67
Readme Files on Your Product Disk	67
Web and Internet Sites	67
Customer Support Technicians	67
Glossary	69
Index	73

1

Introduction

With the growing amount of information that travels on your local area network (LAN), confidential information has become a target for intruders both inside and outside your company. These intruders may be employees, visitors to your company, or a hacker who breaks through your firewall.

Intel® Packet Protect helps protect Internet Protocol (IP) traffic as it travels between computers on your LAN. This protects confidential data from being retrieved by intruders.

In this chapter, you'll find information about:

- Packet Protect overview
- How Packet Protect works
- Getting started

What is Intel® Packet Protect?

Packet Protect is designed to protect the confidentiality and authenticity of IP traffic on your LAN.

Packet Protect can assist you in creating a departmental solution for your security concerns.

Many data compromises are attempted from within a company firewall. Unless you protect information as it travels on the network, it can be received by unwanted users.

For example, employees retrieving confidential designs from a Research & Development department server use Packet Protect to encrypt the information while it travels on the LAN. Encryption protects the confidentiality of the information. Each employee's computer can also verify the integrity of the information upon receipt.

Packet Protect Features

Packet Protect enables you to:

- Protect confidentiality and authenticity of IP traffic on your LAN using Internet Protocol Security (IPSec), including Internet Key Exchange (IKE).
- Offload security tasks to an Intel® PRO/100 S Management or Server Adapter to optimize network performance.

Complete Your Security Solution

If you need to protect data stored on a computer, use operating system features combined with Packet Protect. Packet Protect protects data traveling *between* computers, not while it's stored on a computer. You should use your operating system features or network infrastructure element to provide access control to certain areas of the computers on the network.

Hardware Acceleration

Implementing an IPSec solution can increase CPU utilization for computers that use the IPSec software. This is common when implementing any IPSec solution because of the intense computation required to encrypt, decrypt, and validate packets. However, there is a way to offload security tasks from the CPU.

You can combine Packet Protect with the use of an Intel PRO/100 S Management or Server Adapter to reduce CPU utilization. This frees CPU utilization for other tasks, while reducing the impact to network performance.

Domestic and Export Versions

Packet Protect is available in both domestic and export versions. The export version supports DES (56-bit) encryption only. The domestic version, available in the United States and Canada, supports DES and 3DES (168-bit) encryption.

Additional Information

This *Packet Protect User's Guide* in Adobe Acrobat* format can be found in the Packet Protect directory on the product CD-ROM. Packet Protect help can be found in the Help directory on the product CD-ROM.

How Packet Protect Works

Packet Protect helps you protect network traffic that is sent from one server or client to another. Packet Protect uses these steps to protect information traveling on the network:

1. **Activate IKE** (Internet Key Exchange). Negotiates parameters for secure communication.
2. **Activate IPSec** (Internet Protocol Security). Protects the communication using the security parameters it negotiated successfully using IKE.

What is IP Security?

Internet Protocol (IP) Security (commonly called IPSec) is a set of standard protocols used to protect the confidentiality and authenticity of IP communications. IPSec accomplishes this using the following:

- **Encryption.** Protects confidentiality of information traveling on the network. Each packet is encrypted so that unwanted recipients can't interpret it. Packet Protect uses DES 56-bit and 3DES 168-bit encryption algorithms (3DES in U.S. and Canada version only).
- **Integrity.** Protects the authenticity of the information traveling on the network by verifying that each packet was unchanged in transport. Packet Protect uses MD5 and SHA-1 authentication algorithms for both ESP and AH authentication.
- **Anti-replay protection.** Protects the network by preventing an intruder from successfully repeatedly sending an identical packet in an attempt to confuse the system.

For more information about IPSec, see "Appendix A — IKE and IPSec" on page 53.

What is Internet Key Exchange?

Internet Key Exchange (IKE) is a standard protocol used to negotiate a protected communication. Negotiation is the first phase in setting up a secure communication. IKE verifies the identity of the computers using pre-shared keys. Then it negotiates a set of security settings to protect the communication.

IKE is a protocol that operates inside a framework defined by ISAKMP (Internet Security Association Key Management Protocol) and is used to support the establishment of Security Associations.

For more information about IKE, see "Appendix A — IKE and IPSec" on page 53.

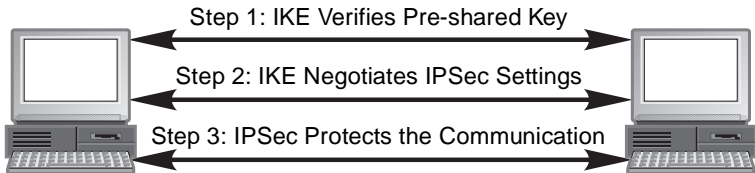
The Process

If two computers require security, each time they attempt to communicate with each other Packet Protect follows these steps to attempt a protected communication:

1. Each computer uses IKE to verify that the other is the computer it claims to be.
2. If identity verification is successful in Step 1, the two computers use IKE to agree upon the IPSec settings to use.
3. If the agreement is successful in Step 2, both computers will use the agreed upon IPSec settings to protect the data as it travels.

As long as the protected communication is active, the two computers can exchange information, without repeating Steps 1 and 2 (up to the pre-defined time and size limits — see Table 6 on page 34 for more information).

The following diagram shows the roles of IKE and IPSec.



Get Started

To start using Packet Protect

1. Evaluate your network architecture and decide which areas require Packet Protect. For details, see “Developing Your Deployment Model” on page 8.
2. Install Packet Protect on those computers that require security. For details, see “Install Packet Protect” on page 17.
3. Set up security settings for each computer where you installed Packet Protect. For details, see Chapter 3, “Configuring Security Settings” on page 21.

2

Installing Packet Protect

To set up your network in preparation for deploying security, there are several things to consider. This chapter guides you through the setup process so you can begin deploying security most effectively.

In this chapter, you'll find information about:

- Developing your deployment model.
- Setting up Intel® network adapters.
- Installing Packet Protect.

Developing Your Deployment Model

In order to use Packet Protect successfully, you must develop a deployment model that fulfills your security needs on your network. There are several stages to consider in developing your deployment model.

- Review your network architecture and corporate security guidelines.
- Assign security behavior roles to computers that you want to use Packet Protect.
- Develop a strategy for using pre-shared keys.
- Understand the Default Rule.
- Consider exceptions to the Default Rule.

This discussion represents only an overview of some of the issues that should be considered when deploying Packet Protect in your enterprise. For more detailed information about deployment models, please refer to “Scalable Deployment of IPSec in Corporate Intranets” white paper from the Intel Architecture Labs Internet Building Blocks Initiative. This white paper can be found at:

ftp://download.intel.com/ial/home/ibbi/ipsec_122.pdf

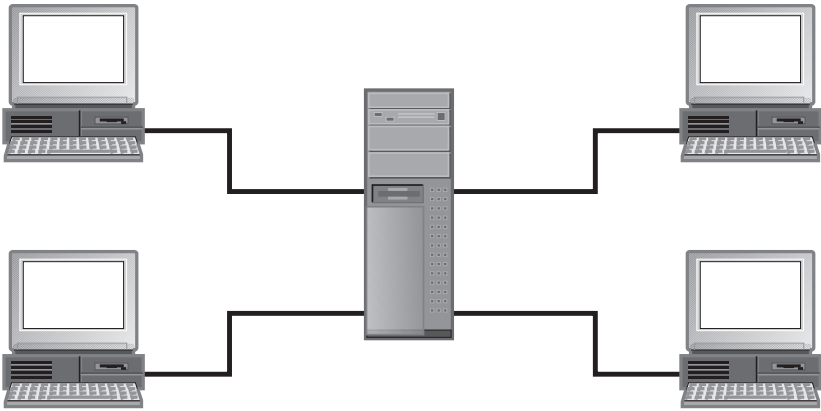
Review Your Network Architecture and Corporate Security Guidelines

The amount of confidential information traveling on your network grows as more employees use your corporate network. This poses a security risk if someone breaks through your firewall, or someone already behind your firewall has access to the network—those people can access confidential information. For example, an intruder can mimic an IP address and receive information that was intended for someone else at that IP address. Or, an intruder can use software to view data as it travels on your LAN.

You can deploy Packet Protect in the areas of your network that transmit sensitive information. Some areas of your network might require the additional protection provided by Packet Protect, while other areas might not. Use your corporate security guidelines to help determine which areas of your network require Packet Protect.

Perhaps you have a server that stores highly confidential information, such as corporate financial figures or e-commerce transactions. You can use your operating system's tools to help protect data stored on the server's hard disk, but what about when other computers access that information? Use Packet Protect

to protect your highly confidential information as it travels to and from the server.



Assign security behavior roles to computers that you want to use Packet Protect

Packet Protect uses default security behavior to determine how a computer will communicate with other computers on the network. There are three default behaviors: Secure Responder, Secure Initiator and Lockdown.

Secure Responder

A computer with the default behavior of Secure Responder always initiates and accepts traffic that is not secured. However, it will accept a secure communication if it is initiated by another computer. Of course, the negotiation will succeed only if one of the proposals in the list offered by the initiator can be matched by the responder.

Secure Responder is a likely behavior for the majority of workstations in a network. Communications will always be allowed in the clear between computers that are Secure Responders or Secure Initiators, but will communicate securely with a computer (usually a server) with Lockdown default behavior.

Secure Initiator

A computer with the default behavior of Secure Initiator will always attempt to initiate secure communications on all outbound traffic. Even if an inbound communication flow is initiated in the clear, the response data flow will cause the computer to initiate a secure session. However, if a secure session cannot be initiated, the computers will fallback to communicating in the clear.

Secure Initiator behavior is appropriate for both workstations and servers. Computers who wish to use peer-to-peer secure communications can use Secure Ini-

tiator behavior. Also, many servers can use this behavior as well, as long as the fallback behavior is acceptable for your network.

Secure Initiator is similar to Secure Responder, except that all outbound traffic will result in an attempt to negotiate parameters for security.

Lockdown

A computer with Lockdown behavior will always initiate and respond securely to all data flows. If the negotiation fails on either computer, then traffic will be denied.

Lockdown behavior is used for servers with high content value, as it requires security for all data transmissions.

Communicating with non-Packet Protect computers

It is common to not use Packet Protect on all the computers in your network. While the security that Packet Protect can provide is beneficial, there are several reasons to limit the computers on your network that use Packet Protect, such as:

- Only a limited number of computers on your network require secure communications.
- In order to minimize CPU utilization, you want to limit use of Packet Protect to computers that already have PRO/100S Management or Server adapters.

Computers that use the default behavior of Secure Responder or Secure Initiator will always be able to communicate in the clear with computers in your network that do not use Packet Protect.

Computers that use the default behavior of Lockdown will not be able to communicate with computers in your network that do not use Packet Protect.

Develop a strategy for handling pre-shared keys

When two computers attempt secure communication, they negotiate parameters for the communication. In addition to using their default behavior, described in the previous section, they also exchange a string of characters known as a pre-shared key.

When the computers begin to negotiate parameters, they compare their pre-shared keys. If both computers have the same pre-shared key, then the computers will go ahead and negotiate parameters for the session. If the computers have a different pre-shared key, then the negotiation for secure communication will cease.

Once the pre-shared keys have been compared and matched between the two computers, the IKE protocol generates secure, secret session keys. No one can find out what these session keys are, even if they know what the pre-shared key is. Although pre-shared keys are sometimes called passwords, they do not act like passwords. Even when you know what the pre-shared key is, you cannot use that key to intercept or decrypt the information that is being transmitted.

Sharing keys

It's important when you are developing your deployment model that you decide how to handle the distribution of the pre-shared key. Some networks use a widely-published key, known as a "group key" or the "pre-shared key on the wall." In this strategy, you make the pre-shared available to everyone. This way, all computers will be configured to use the same key. This ensures that when secure communications are requested, then IKE will be able to negotiate secure communications when the keys are matched between two computers.

In addition to "group key," some enterprises may want to use additional, more private pre-shared keys in certain instances. For example, the president and the chief financial officer of a corporation may wish to send secured transmissions to each other. In this instance, each of these computers would use the group key as part of their standard System Policy, but would create a special rule to cover communications just between them. (See "Consider exceptions to the Default Rule" for more information on implementing this scenario.) In this case, they might likely choose a more secret pre-shared key that just the two computers use with each other.

Understand the Default Rule

Every computer that uses Packet Protect has a single System Policy. Each System Policy initially contains a single Default Rule. The Default Rule is quite simple:

For Everybody, use the Default Security Action. If the rule fails, Allow Communication without Security.

Note: For computers that use the Lockdown behavior with the Default Rule, if the rule fails then *Deny Communication* is the fallback action.

See "The Default Rule" on page 26 for more information.

Note: If you want to have secure communication between a Packet Protect computer and a Windows 2000* computer, you must use the Default Rule. Intel recommends that you do not delete the Default Rule.

See "What is a Rule?" on page 25 for more information about rules in Packet Protect.

Consider exceptions to the Default Rule

Many enterprises may find that by careful consideration of the default behavior roles, a widely published pre-shared key, and the Default Rule, they can meet their security requirements without extra effort. This model is quite workable and provides adequate security. It is also simple to deploy and maintain.

Some enterprises may wish to create additional rules that govern communications between two specific computers.

Earlier, we introduced a scenario where the president and chief financial officer of a company wished to implement extra security for their communications. For this scenario, a new rule is needed. Let's compare a possible rule for this scenario to the System Policy's Default Rule:

Table 1: Rule Comparison

Property	New Rule	Default Rule
Destination Workgroup	President and CFO only	Everybody
Security Action	New Security Action: Up to 15 minutes or 50 MB, whichever occurs first. Then, a new security association is negotiated.	Default Security Action: Up to 8 hours, then a new security association is negotiated.
Rule Failure	Deny Communication.	Allow communication in the clear.
Authentication	Use a new pre-shared key, known only to these two computers.	Use the System Policy's settings

In addition to these rules, both the president and the Chief Financial Officer would have the Secure Initiator default behavior. The rule might also want to use more secure options, such as perfect forward secrecy, which provides a very secure negotiation of session keys. There are many other security options that can be chosen when you create a security action for this rule. See “Customize Security Actions” on page 33 for more information on options for security actions.

By comparing the new rule and the default rule, you can see how the new rule provides an extra measure of security. The new security action is much more limited. Longer time and/or size limits on a security action can give an intruder an opportunity to intercept and possibly corrupt packets. By denying communication in case of rule failure, you ensure that communication between these two computers will never occur in the clear.

What are the Trade-offs?

A very important part of developing your deployment model is to consider not only the initial deployment, but maintaining the System Policies on all the computers that use Packet Protect in your network.

Clearly, the simplest model we discussed will be the easiest to deploy and maintain. When all computers use the same defaults—Default Rule, security action,

fallback to clear communication, same pre-shared key—then you'll be able to gain adequate security with minimum impact to your network.

If you decide on a more complex deployment model, you should consider the benefits of the extra security that you have against the costs of maintaining and running the model. There are two areas that you should evaluate—maintenance and CPU utilization.

Maintenance

If you are considering a deployment model with many customizations and specialized rules, be aware of the time and effort required for ongoing maintenance. Because each computer with Packet Protect must be configured individually, customizations require more effort to keep each computer up-to-date.

Let's consider the previous example of the special rule for the president and Chief Financial Officer of the corporation. In order for this rule to work as designed, all aspects of the rule must match, or communication will be denied. If the president's computer uses a different setting in the security action from the CFO's computer, then a security association cannot be negotiated and therefore all communication is denied. Consider then that it might take several days for the president and CFO to even discover that their communications haven't been taking place, as assumed.

Even a new computer for the president could prevent secure communication from happening. For example, when you set up this special rule, you identified the two computers to Packet Protect by the names of the computers. The president's new computer has a new name. When the president and the CFO attempt to communicate the next time, the rule will fail, because of the computer name.

You can imagine how difficult it can become to maintain specialized rules, destination workgroups, and security actions in your network. Intel recommends that you begin by using the simple, default model for secure communications. Over time, you may consider customizations to enhance secure communications in special cases.

CPU Utilization

Another very important factor to consider is the effect of IPSec on your network, as well as the individual computers using Packet Protect. Generally, you can assume that when you choose most sophisticated security options, there will be impact on your network.

One example is choosing to use ESP (Encapsulation Security Payload) and AH (Authentication Header) authentication together. While this combination affords extra protection, you must consider that when you use both of these methods, you cannot offload any processing to the adapter, and thus CPU utilization increases. However, if you use just ESP authentication with the appropriate adapter, you can take advantage of the hardware offload and get better CPU utilization.

You must also consider the adapters that are installed in your Packet Protect computers. Only the Intel PRO/100 S Server Adapter and Intel PRO/100 S Man-

agement Adapter can perform hardware offloading. If you have other Intel PRO/100 Adapters in Packet Protect computers, you won't be able to offload any processing, thus increasing CPU utilization and potentially slowing that computer's network performance.

Other security options are considered "costly" as well. Perfect Forward Secrecy is very secure, but if used widely throughout the network, there can be a significant effect on servers that have a lot of secure traffic.

Conclusion

Hopefully, this section provided some guidelines for you to consider as you develop your deployment model. There are no hard-and-fast rules that you must follow. However, Intel recommends that you begin your use of IPSec and Packet Protect slowly in your enterprise. You should consider starting with a small group that use the same pre-shared key and default System Policy. When you've had a chance to evaluate this first implementation phase, you can then decide how to expand your use of Packet Protect.

Set Up Intel Adapters

Before you install Packet Protect, install the necessary Intel adapters on your servers and clients that will use Packet Protect. Packet Protect only operates with Intel adapters that are configured to use Intel drivers.

Install Intel Adapters

Packet Protect works with Intel adapters that are designed to offload CPU-intensive tasks to the adapter. This helps reduce the impact to network performance and CPU utilization. Intel adapters that support the offload capabilities include the following:

- Intel PRO/100 S Server Adapter
- Intel PRO/100 S Management Adapter

Note: Although Intel adapters can be installed on various operating systems, Packet Protect supports only Windows NT* 4.0 with Service Pack 5.

Note: Packet Protect also works with the following Intel adapters, but security tasks will not offload to these adapters, and network performance will be affected.

PRO/10+ PCI LAN adapter
 PRO/100B LAN adapter
 PRO/100B T4 LAN adapter
 PRO/100+ LAN adapter
 PRO/100+ Management adapter
 PRO/100+ Server adapter
 PRO/100+ Dual Port Server adapter
 PRO/100 CardBus II
 PRO/100 RealPort™ CardBus II
 PRO/100 LAN+Modem56 CardBus II
 PRO/100 LAN+Modem56 RealPort™ Cardbus II

Install Intel adapters for the servers and clients that use Packet Protect.

To install Intel adapters

1. Refer to the *Installation Guide* that came with the adapters for information about installation
2. After installation, verify network access for each computer that will use Packet Protect by checking the Link and Activity LEDs on the adapter. You can also double-click Network Neighborhood on a computer's desktop to verify that other areas of the network are visible.

Configure Intel Adapters

After you install adapters in the computers that will use Packet Protect, configure them, as necessary, before you install Packet Protect. For example, you

might install multiple adapters on a server. Then you might team those adapters together to take advantage of adapter fault tolerance or adaptive load balancing.

Multiple Adapters

If you install multiple adapters in one computer, note the following:

- Install multiple adapters before installing Packet Protect.
- Each computer has only one security policy. This means that the same security settings will apply to all of the adapters in one computer.
- If you use at least one Intel PRO/100 S Server or Management adapter in a computer, Packet Protect will be able to offload encryption and authentication tasks to that adapter.
- If you need to add or remove an adapter from a team after you install Packet Protect, you must uninstall Packet Protect from that computer, add or remove the necessary adapters, and then reinstall Packet Protect.

When you uninstall Packet Protect, you lose all of your customized information, including rules and security actions. When you reinstall Packet Protect, you will only have the single Default Rule in your System Policy.

Adapter Teaming

Adapter Teaming and Packet Protect work together only for computers with Windows NT operating system installed. If you set up Adapter Teaming for multiple adapters, keep the following in mind:

- Configure Adapter Teaming before installing Packet Protect.
- Refer to the previous page to make sure all adapters in the team are either offload-enabled Intel adapters, or appear in the list of compatible Intel adapters on the previous page.
- If you need to add or remove an adapter from a team after you install Packet Protect, you must uninstall Packet Protect from that computer, add or remove the necessary adapters, and then re-install Packet Protect.
- Consider using high-speed adapters to limit upgrading.

Install Packet Protect

Before you install Packet Protect on your computer, make sure the computer meets the following system requirements. Packet Protect computers can be servers or workstations.

System Requirements

Before installing Packet Protect, make sure your computers meet these requirements:

- Windows NT 4.0 with Service Pack 5 or 6a (or higher)
- 40 MB available disk space
- 32 MB RAM minimum, 64MB RAM recommended
- 200 MHz Pentium® processor performance level or higher recommended
- Intel adapter (PRO/100 family)

Note: See “Install Intel Adapters” on page 15 for information on choosing an Intel adapter.

Licensing

All installations are subject to the end user’s acceptance of the applicable Intel Software License Agreement.

Install Packet Protect

You will need the information detailed in the following table during Packet Protect installation at each computer. To complete the installation most efficiently, gather the following information before you begin.

Table 2: Required Information

Information You Need	Description
Default behavior	Decide how you want the computer to communicate with other computers on the network: <ul style="list-style-type: none"> • Secure Responder • Secure Initiator • Lockdown For more information about these settings, see “Default Behaviors for Packet Protect Computers” on page 22.
Pre-shared key	Enter a pre-shared key the computer will use to communicate securely with other IPSec computers. A pre-shared key is similar to a secret password.

To install Packet Protect

1. Verify that the computer you have chosen meets the minimum requirements detailed under “System Requirements” on page 17.
2. Insert the product CD-ROM into the CD-ROM drive at the computer where you want to install Packet Protect.
3. Browse to the CD-ROM using Windows Explorer.
4. Double-click `d:\packet protect\setup.exe`, where `d:\` is the drive of your CD-ROM drive.
5. Follow the dialog box instructions on the screen.

Keep a confidential record of the information you enter. If you need to reinstall Packet Protect later, you will need to re-enter this information.

Notes: If the static IP address or the DNS name of the computer changes, you must restore the System Policy. You will lose all your customizations when you restore the System Policy. Also, if there are other computers in the network that have rules that apply to the computers whose IP address or DNS name changes, the rules of those computers need to be changed. For information on restoring the System Policy, see “Restore the System Policy” on page 42.

You can also install from a mapped drive where you have stored the Packet Protect installation files.

If you already have adapter teaming installed on the system, there's no need to re-enter the TCP/IP settings during Packet Protect installation (you are not prompted for this information).

To verify that Packet Protect is installed and running on a computer:

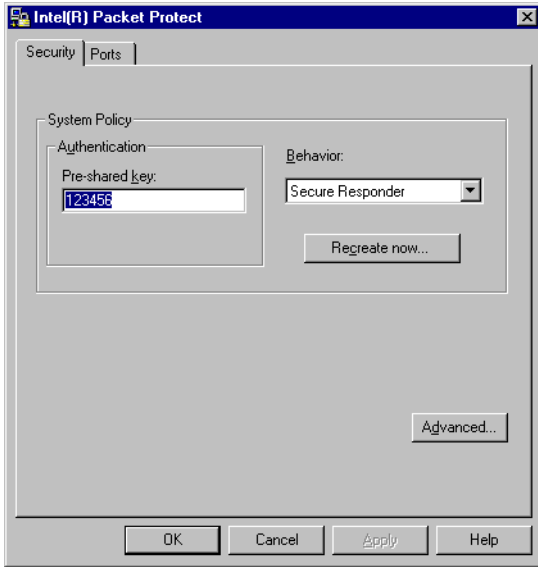
1. At the taskbar on the computer, select **Settings > Control Panel**.
2. Double-click **Services** and verify that **Intel Policy Agent** is started.

If Intel Policy Agent doesn't appear in the list, Packet Protect has been shut down or is not functioning properly. See “Turn Security on Manually for an Existing Computer” on page 47 for details about restarting Packet Protect.

See the chapter “Troubleshooting and FAQs” on page 49 for general troubleshooting guidelines and a list of common Packet Protect installation problems and their solutions.

View Your Security Settings

During installation, you set up basic security settings for the computer—the authentication method and the default behavior for the client. To view your security settings, double-click Intel(R) Packet Protect at the Control Panel. The authentication setting and default behavior you chose during installation appear in the Security tab.



See the next chapter for information on editing basic settings and configuring advanced security settings.

3

Configuring Security Settings

If you have installed Packet Protect, you have already set up basic security settings for the computer. You may view or edit these settings using Packet Protect. Optionally, you may also use the Advanced settings in Packet Protect, if you are familiar with encryption and authentication settings, to configure the security policy that comes with Packet Protect.

In this chapter, you'll find information about:

- Understanding default security behavior (basic settings).
- Setting up your System Policy (advanced settings).

Understand Default Security Behavior

During installation, you selected a default behavior for your computer to use for all communications. You also entered a pre-shared key that matches the pre-shared key on other computers in the network so the computer can communicate securely with other computers possessing the same pre-shared key.

Default Behaviors in Packet Protect

In order to operate with security settings, your computer needs to know how to communicate with other IPSec-enabled computers. In the absence of a rule that matches a specific communication need, Packet Protect uses default behaviors to determine how IPSec computers use security. If a matching rule exists on the two computers that are attempting to communicate, the default behavior will not be used. The table below describes the default behaviors available with Packet Protect.

Notes: You can set up specific security policies with rules to apply to specific types of communications using advanced security settings. See “Set up Your System Policy” on page 25 for more information.

You cannot make any changes to Packet Protect on a computer unless you are logged on as *administrator*. Individual users cannot modify Packet Protect settings.

Table 3: Default Behaviors for Packet Protect Computers

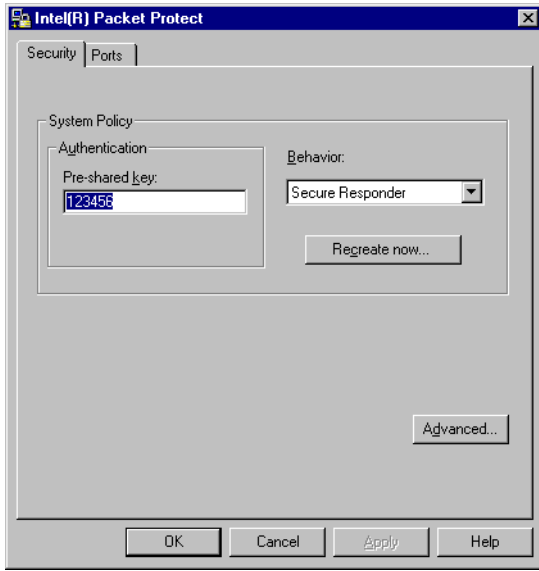
Default Behavior	Description
Secure Responder (Example: workstations)	<p>Computers with this behavior initiate communication without security (in the clear), but will attempt to negotiate a secure communication if one is requested. For example, if a Secure Responder workstation attempts to access a file server and that file server requests a secure communication, the workstation will respond in a secure manner.</p> <p>If two workstations are configured with this setting and they attempt to communicate with each other, the communication is allowed without security (in the clear). Also, Secure Responders and computers that are not IPSec-enabled communicate without security.</p>

Table 3: Default Behaviors for Packet Protect Computers

Default Behavior	Description
Secure Initiator (Example: servers)	Computers with this behavior request security for all communications, but don't require it. For example, a Secure Initiator server always initiates communications by requesting security. If the negotiation for a secure communication is unsuccessful, the Secure Initiator server communicates without security (in the clear).
Lockdown (Example: servers that require strict security)	<p>Computers with this behavior <i>require</i> security for <i>all</i> communication. Lockdown computers do not communicate without security, that is, they do not communicate in the clear.</p> <p>Only use Lockdown if a computer will be accessed by a very limited number of computers, and those computers are all properly set up with Packet Protect. If a backup to another computer on the network is scheduled automatically, it will fail unless the other computer is also security-enabled.</p>

To change the default behavior for a Packet Protect computer

1. Click Start > Settings > Control Panel.
2. Click Intel® Packet Protect. The Packet Protect Security tab appears:



3. To change the behavior for your computer, use the Behavior drop-down list to choose one of these behaviors: Secure Responder, Secure Initiator, or None.
4. To change the pre-shared key, type a new key in Pre-Shared key box.
5. When you are finished viewing and making changes in the Security tab, click OK.

Set up Your System Policy

You set up basic security settings when you install Packet Protect. If you are familiar with encryption and authentication settings you can use the advanced settings in Packet Protect to configure specific security settings to apply to different types of communication. Packet Protect comes with a system policy that contains advanced security settings.

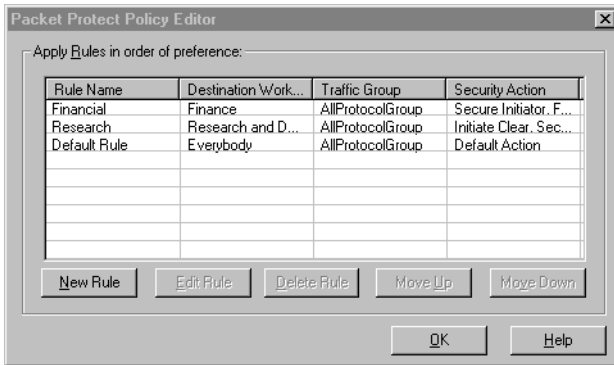
What is a Policy?

A policy helps determine how the computers you manage communicate with each other and with other computers on the network. Policies contain one or more rules and use rules to specify how computers on the LAN communicate in a protected way. Your Packet Protect policy comes with pre-defined rules. Each rule has its own set of conditions that, if matched, apply defined security settings. You can edit the pre-defined rules or create new rules for your policy.

What is a Rule?

A rule defines how you want to communicate with other computers on the network. For example, one rule can define how to communicate with a file server using specific security settings. Another can define an entire group of computers for which communication will always be allowed “in the clear” (without security).

The rules in your system policy are listed in the Policy Editor. To view the Policy Editor, click Advanced on the Security Tab.



Every rule contains the information described in the following table.

Table 4: Rule Settings

Rule Setting	Description
Destination workgroup	Collection of computers with which a computer communicates.
Security action	Collection of security settings used when negotiating a communication.
Rule failure	Definition of what happens when the rule is applied, but the communication is not negotiated successfully. You can allow the communication to occur unsecured, or deny the communication.
Authentication	Definition of how your computer verifies the other computer's pre-shared key when the rule is applied. You can use the authentication settings already specified for your computer (on the Security tab), or use custom settings for the rule (propose a pre-shared key).

Note: All rules specify All IP for the Traffic Group. If a rule is applied, the security settings apply to all IP traffic between the two computers communicating. Refer to the readme file on the product CD-ROM for a list of ports and protocols that are always sent unprotected in order for Packet Protect to function.

The Default Rule

When you install Packet Protect, the default rule is created. The Default Rule has these properties:

- Destination Workgroup *Everybody.*
Applies to every computer in the LAN.
- Security Action *Default Action.*
The standard security action, which uses a time limit of 8 hours. Refer to “Customize Security Actions” on page 33 for detailed information about security actions.

- If rule fails *Allow Communication without Security.*
If the computers cannot negotiate a secure communication, then communication is allowed without any security. For computers that use the Lockdown behavior—if the rule fails, then communication is denied.
- Rule authentication *Use System Policy's settings.*
When Packet Protect was installed, each computer was set up to use a pre-shared key. When two computers attempt to communicate securely using a pre-shared key, each computer must have the same key entered. If these keys do not match, the rule cannot be authenticated by the computers and it will fail.

Importance of Rule Order

The System Policy typically contains one or more rules. Place the rules in the order you want them applied. If you have one general rule and also an exception to that rule, place the exception before the general rule; otherwise, the specific rule is never applied.

It is critical that you order rules appropriately to ensure they behave as expected. The following example shows what might happen if the rules are not in the correct order.

Example of rule ordering

Suppose you have created a destination workgroup for the finance managers at your company. You need to send sensitive information to the managers, so you have created a rule with high security settings. You decide that if one of the finance managers does not meet the security action settings, you do not want to transmit information. You also have the Default Rule with security settings to use when communicating with everyone on the LAN. However, if the settings fail to be negotiated, you will still allow the communication to take place without security. The rules you have created appear in the table below.

Table 5: Correct Ordering for Rules

Rule Name	Destination Workgroup	Security Action	If rule fails
To Finance Management	Finance Managers	3DES+SHA1+None	Deny
Default Rule	Everybody	DES+MD5+None	Allow

The rule ordering above requires the Finance Managers workgroup to have a rule listing your computer and the 3DES+SHA1+None security action in order to negotiate secure communication. If the Finance Managers workgroup does not have a matching rule, communication will be denied.

Notice the importance of rule order. If the Default Rule was ordered before the *To Finance Management* rule, communication with Finance manager workstations would be allowed “in the clear” (with no security) even if the Finance Managers workgroup does not have a matching rule for communication with R&D using the 3DES+SHA1+None algorithms. In this case, the general rule would be applied first, and the specific rule would never be applied.

For instructions on how to order rules, see “Step 3: Order the Rules” on page 31. The next section explains more about how Packet Protect computers use rules.

For information about security algorithms and about their notation, see “About algorithm notation” on page 36.

How Does the System Policy Work?

The System Policy defines a collection of rules that describes the security settings to enforce under certain situations. When a computer attempts communication, Packet Protect evaluates a number of things before allowing the communication.

The following example describes how the policy works:

1. MyComputer attempts to communicate with MyServer with a rule using the 3DES+SHA1+None encryption algorithms.
2. ***If a rule match is found***, MyComputer proposes the security action settings and authentication settings that you defined for that rule. The two computers negotiate the security settings. If that security settings negotiation is successful, the two computers communicate using the agreed upon settings. If that negotiation fails, the communication fails or is allowed unsecured, depending on the *if rule fails* specification.
If a rule match isn't found, the system proposes the pre-shared key assigned for that computer's workgroup. It then proposes pre-defined security settings such as default settings that are used for all communications. See “Appendix A — IKE and IPSec” on page 53 for more information.

Note: If the destination computer uses Packet Protect, it also searches its policy for a rule with settings that match. If your computer and the destination computer have matching rules, the communication is allowed secure according to the specified security action settings.

Add Rules to the System Policy

Adding rules to your policy is optional. If you are unsure whether you need new rules, see “What is a Policy?” on page 25 for more information.

Creating a new rule involves several steps:

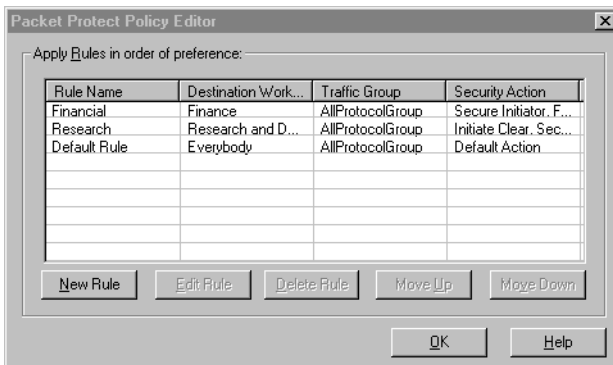
1. Viewing the System Policy.
2. Defining a new rule for the System Policy.
3. Ordering the rules.

In general, follow these guidelines when you make rules:

- When you add a rule to computer A's policy for secure communication with computer B, you must add a matching rule in computer B's policy for secure communication with computer A. Otherwise, the rule will fail and communication will be denied or allowed unsecure (depending on the *If rule fails* setting for both workgroups' rules).
- If you add two rules that include some of the same computers (for example, one rules lists computer A as the destination workgroup, and another rule lists Everybody – all computers on the network – as the destination workgroup), you must order the specific rule before the general rule. Otherwise, the specific rule will never be applied. See “Importance of Rule Order” on page 27 for more information.

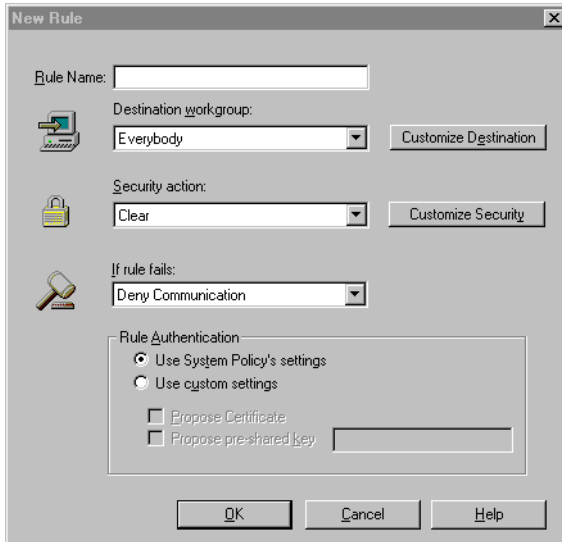
Step 1: View the System Policy

1. At the Control Panel, click Intel Packet Protect.
2. On the Security tab, click Advanced... . The Policy Editor dialog box appears:



Step 2: Define a new rule for the policy

1. Click New Rule. The New Rule dialog box appears.



2. In the Rule Name text box, type a name for the rule.
3. In the Destination workgroup text box, select the group of computers for which you want this rule to apply.

The list includes destination workgroups that are already created (either as part of the Default Rule or that you created). If you want to view, edit, or create a destination workgroup, see “Customize Destination Workgroups” on page 31 for more information.
4. In the Security action text box, select the group of security settings that you want to define for this rule.

The list includes security actions you have already created and pre-defined security actions that come with Packet Protect. If you want to view, edit, or create a security action, see “Customize Security Actions” on page 33 for more information.
5. In the If rule fails text box, select whether to deny or allow a communication if this rule is matched, but the communication fails to negotiate.
6. In the Authentication area, decide whether you want to use the default settings or propose custom authentication settings.

You specified the default settings when you installed Packet Protect (displayed on the Security tab).
7. Click OK.
8. Repeat steps 2 through 7 to add more rules to the System Policy.

Step 3: Order the Rules

1. On the Policy Editor dialog box, click a rule.
2. Click Move Up or Move Down to move the rule up or down one line. You can also select a rule and drag it up or down.

The rules are applied in the order in which they are listed. The rule at the top of the list is applied before all rules below it, for example.

See “Importance of Rule Order” on page 27 for more information about ordering rules.

To modify a rule

In order to apply your rule to a communication, the computer with which you are attempting communication must have a rule with matching settings. If you have already coordinated rules with the other computers with which you wish to communicate, modifying your rule will require modification to rules for other computers.

1. Before you modify a rule, check the following:
 - If you have already set up matching rules for other IPsec computers, DO NOT follow the steps below.
 - If you have not set up matching rules for other IPsec computers, continue with the steps below.
2. In the Policy Editor dialog box, select rule you want to modify.
3. Click Edit Rule. The Edit Rule dialog box appears.
4. Make changes, as necessary, then click OK.

Customize Destination Workgroups

A destination workgroup is a collection of computers with which your computer communicates. For example, if your computer requires specific security when communicating with the Research & Development Workgroup, your policy must include a rule with security settings that specifies the Research & Development Workgroup as the destination workgroup, and Research & Development computers must have a rule specifying the same security settings and your computer as the destination workgroup.

The following destination workgroups are available:

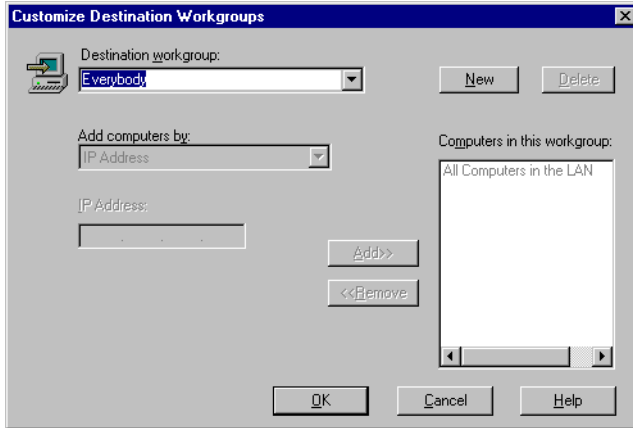
- Everybody: Use this destination workgroup when you want the rule to apply to communication with all computers on your LAN.
- Destination workgroups you create.

If a computer or group of computers you need is not in the destination workgroup list, create a new destination workgroup.

To create a new destination workgroup

1. On the Policy Editor dialog box, select the rule for which you want a new destination workgroup.

2. Click Edit Rule. The Edit Rule dialog box appears.
3. Click Customize Destination. The Customize Destination Workgroups dialog box appears.



4. Click New.
5. In the Destination workgroup box, type a new name for the destination workgroup.
6. To add computers to the destination workgroup, in the Add computers by text box, select how you want to identify computers for addition to the destination workgroup: by IP address or by computer name.

Note: Check with your network administrator to determine how to add computers to a workgroup. If the computer you want to add to this workgroup has a permanent (or static) IP addresses, you should probably add computers to the workgroup by IP address. If the computer you want to add uses dynamic IP addresses (where a temporary IP address is assigned to a computer for each session), then you should probably add computers to the workgroup by computer name.

7. Type the computer name or IP address for a computer you want to add to the workgroup.
8. Click Add>>.
9. Repeat steps 5 through 8 for each computer you want to add.
10. If you need to delete a computer from the destination workgroup, select the computer from the list on the right, then click <<Remove.
11. If desired, continue adding destination workgroups by clicking New again and repeating Steps 4-7.
12. Click **OK**. The selected destination workgroup appears automatically in the Edit Rule dialog box.

Destination workgroups can be used in multiple rules. If you modify a destination workgroup, other rules may be affected.

Before you modify a destination workgroup, check the following:

- If you have used the destination workgroup in any other rules, do not follow the steps below. See “Modify Destination Workgroups or Security Actions” on page 41 for more information.
- If you have not used the destination workgroup in any other rule, continue with the steps below.

To modify a destination workgroup

1. In the Customize Destination Workgroups dialog box, select the destination workgroup you want to modify.
2. Make changes, as necessary, then click OK.

Customize Security Actions

You must specify a security action for each rule. This section defines the security settings you can apply when two computers communicate.

Packet Protect provides six pre-defined security actions, described below. See “Available Settings for Security Actions” on page 34 for detailed information about the security settings listed here.

- **Clear**
Use to communicate completely in the clear, without any security.
- **Default Action**
Use to get an action that provides a high level of security, along with a high level of interoperability. The default action is a rich set of IPSec proposals that includes various levels of ESP (Encapsulation Security Payload) encryption, ESP authentication, and AH authentication. It provides a maximum level of interoperability with non-Packet Protect implementations of IPSec.
- **Deny**
Use to deny any communications between two computers.
- **Initiate Clear, Secure Responder**
Use when you want to initiate communications in the clear and will attempt to negotiate a secure connection if requested. This security action is most appropriate for workstations.
- **Secure Initiator, Fallback Clear**
Use when you want to request security for all communications, but do not require it. If a secure connection cannot be negotiated, then the communication will be in the clear. This security action is appropriate for servers.
- **Secure Initiator, Fallback Deny**
Use when you want to require security for all communications. If a secure

connection cannot be negotiated, then the communication request is denied. This security action is appropriate for servers.

Remember that two computers attempting to communicate must agree on certain settings in order to communicate using IPSec.

The *Requires Match?* column in the table below indicates whether the source and destination computers must have the same security setting..

Table 6: Available Settings for Security Actions

Security Setting	Description	Requires Match?
Time limit	<p>The length of time (in minutes or hours) the protected communication can be active before the system renegotiates. To increase protection, lower the time limit (to a minimum of 10 minutes). This makes the system renegotiate a new security association more often, but increases network traffic. You may specify a time limit, size limit, or both. This setting is optional.</p> <p>If two computers require different time limits, the communication is re-negotiated when the lower time limit is reached. If a time limit is not defined, the default is 8 hours.</p>	No
Size limit	<p>The amount of data (in MB) that can be transferred during a security association before the system renegotiates. To increase protection, lower the size limit (to a minimum of 20 MB). This makes the system renegotiate a new security association more often, but increases network traffic. You may specify a time limit, size limit, or both. This setting is optional.</p> <p>If two computers attempting to communicate require different size limits, the security association expires when it reaches the lower size limit. If you specify a size limit only, an 8-hour time limit is applied automatically. The default is no size limit. There is no maximum size limit for a security association.</p>	No

Table 6: Available Settings for Security Actions

Security Setting	Description	Requires Match?
Perfect forward secrecy	<p>The system proposes a second set of keys for the security association (instead of using the first set of keys used to verify identification). Packet Protect is designed to agree on any of the settings (including none), but it proposes the setting you select.</p> <p>Note: DO NOT use perfect forward secrecy if your computers will need to communicate securely with Windows* 2000 IPSec computers or any other non-Packet Protect IPSec computers. This setting is not compatible with non-Packet Protect IPSec computers and may cause communication to fail.</p>	No
Anti-replay protection	<p>The system does not accept repeated packets; that is, packets that the system already received. This helps protect against an intruder sending the same packets repeatedly in an attempt to confuse an application. Always use this option because it increases the level of protection with very little impact on network traffic.</p>	No
Use algorithms in order of preference	<p>Combinations of algorithms a computer must use for a communication: ESP encryption, ESP authentication, and AH authentication. Packet Protect proposes the algorithm list (in order of preference) to the destination computer during negotiation. <i>Two computers attempting to communicate securely must agree on an algorithm combination.</i></p>	Yes

Note: If your computer needs to communicate securely to a mixed domestic and export group of computers, make sure your policies have compatible encryption settings. Computers using the export version can use DES encryption only. If computers using the export version receive a policy specifying 3DES encryption, they will actually use DES encryption for the communication. Consider including both DES (56-Bit) and 3DES (168-Bit) encryption in your security actions.

About algorithm notation

Each security action can specify algorithms to use for encryption and authentication. There are three categories (Encryption, ESP [Encapsulation Security Payload] Authentication, and AH [Authentication Header] Authentication).

At least one of these categories must be used in a security action, or you can use two or even all three.

IPSec and Packet Protect use a kind of “shorthand” notation for describing the algorithms used in a security action—Encryption value + ESP value + AH value. For example, if you create a security action that uses DES for Encryption, SHA1 for ESP, and do not use AH, this would be shown as DES+SHA1+None.

To create a new security action

1. On the Policy Editor dialog box, select the rule for which you want a new security action.
2. Click Edit Rule. The Edit Rule dialog box appears.
3. Click Customize Security. The Customize Security Actions dialog box appears.
4. Click New.
5. In the Security action list box, type a new name for the security action.
6. Specify a time and/or size limit for the security association. Refer to Table 6, “Available Settings for Security Actions,” on page 34 for detailed information about these items.
7. If applicable, select the Perfect Forward Secrecy check box.

Note: DO NOT use Perfect Forward Secrecy if your computers will need to communicate securely with Windows 2000 IPSec computers or any other non-Packet Protect IPSec computers.

8. Select Anti-replay protection. (Always select this setting because it increases network protection with very little impact on network traffic—see Table 6 on page 34 for details.)
9. Add algorithms to the preference list for the security action:
 - In the Encryption, ESP Authentication, and AH Authentication list boxes, select which algorithms you want to propose for the security action. You must select at least one algorithm from any of the lists.
 - Click Add.Repeat this step for each algorithm combination you want to add.
10. If you need to remove an algorithm combination from the preference list, select the combination from the list on the right, then click Remove.
11. To indicate your order of preference, move the algorithm combinations to the correct location on the list by selecting an algorithm combination and clicking Move Up or Move Down. Move the most important selection to the top of the list and continue in descending order of importance.

12. To continue adding security actions, click New again and repeat Steps 5-11.
13. When you finish, click OK. The selected security action appears automatically in the New Rule dialog box.

To modify a security action

Security actions can be used in multiple rules. If you modify a security action, other rules may be affected.

1. Before you modify a security action, check the following:
 - If you have used the security action in any other rules, DO NOT follow the steps below. See “Modify Destination Workgroups or Security Actions” on page 41 for instructions.
 - If you have not used the security action in any other rule, continue with the steps below.
2. In the Customize Security Action dialog box, select the security action you want to modify.
3. Make changes, as necessary, then click OK.

4

Making Changes

Be careful when you make changes to your policy. The settings you modify may be used for more than one rule in your policy. This means changes you make may affect other rules in your policy, and may even require changes to policies for other Packet Protect computers.

In this chapter, you'll find information about:

- Modifying rules.
- Modifying custom destination workgroups and custom security actions.
- Deleting rules.
- Restoring the system policy.

Modify the System Policy

Modifying a computer's System Policy may impact policies that belong to other clients with which your computer communicates using Packet Protect. In order to apply your rule to a security association, the computer with which you are attempting communication must have a rule with matching settings. If you have already coordinated rules with these other computers, modifying your rule will require modification to the rules for the other computers. Contact the network administrator if you have any questions or concerns about modifying rules in the System Policy.

You may edit the Default Rule that comes with your Packet Protect System Policy (see "The Default Rule" on page 26 for a description of the Default Rule).

Notes: You should carefully consider the possible effects of changing the Default Rule. If you modify the Default Rule extensively on a computer, then you run the risk of that computer not being able to successfully negotiate a secure transmission with another computer in your network.

If you have to re-install Packet Protect for any reason, or need to recreate the Default Rule, you will lose your customizations and will have to specify them again.

To modify a rule

1. Determine which of the other computers on the LAN have a matching rule for the rule you will edit. You need this information later.
2. On the Policy Editor dialog box, select the rule you want to modify.
3. Click Edit Rule. The Edit Rule dialog box appears.
4. Make changes as necessary.
5. If you click any of the Customize buttons to make changes, see "Modify Destination Workgroups or Security Actions" for more information.
6. Click OK.
7. Go to the other computers that have a matching rule for the rule you just modified (if you do not administer the other computers, coordinate the needed rule changes with the other administrator). Complete steps 2-6 on each of the other computers to update the settings so the rules have matching settings.

Note: You must change matching rules on other computers when you modify your rules. Otherwise, when the computers attempt to communicate, the rule may fail and the security settings are not used.

Modify Destination Workgroups or Security Actions

Destination workgroups and security actions can be used in multiple rules. If you modify these items, other rules may be affected. Follow these steps to ensure that you address other affected rules.

Determine which other computers on the LAN have a matching rule for the rule you will edit. You will need this information later.

To edit destination workgroups or security actions:

1. Determine which other rules that use the destination workgroup or security action you wish to modify. You will need this information later.
2. On the Policy Editor dialog box, select the rule containing the destination workgroup or security action you want to edit.
3. Click Edit Rule. The Edit Rule dialog box appears.
4. Click Customize Destination or Customize Security, depending on what you want to edit. The appropriate dialog box appears.
5. Select the item you want to modify.
6. Make changes as necessary.
7. When you are finished, click OK.

Any rule that uses the destination workgroup or security action you just modified will also use the modified settings.

8. Administer the other computers that have a rule matching any of the rules that use the modified destination workgroup or security action. (If you do not administer the other computers, coordinate the needed rule changes with the other administrator.) Complete steps 2-7 to update the settings in the matching rule.

Note: You must change matching rules on other computers when you modify your rules. Otherwise, when the computers attempt to communicate, the rule fails and the security settings are not used.

Delete a Rule

Caution: After you delete a rule, you cannot recover its information.

To delete a rule:

1. On the Policy Editor dialog box, select the rule you want to delete.
2. Click Delete Rule.
3. Click Yes to confirm the deletion.

Note: If other computers have a rule that matches the one you just deleted, you should delete the matching rule in the System Policy of those computers.

Restore the System Policy

If the System Policy on your computer has been extensively modified, you may find that your computer can not always negotiate a secure communication with another computer on the LAN.

When this occurs, you should consider removing your customizations and returning to the original System Policy, with its Default Rule. You will lose all of your customizations, including customized destination workgroups and security actions.

To restore the System Policy

1. Display the Intel Packet Protect Security Tab.
2. Click Recreate Now. All your customizations are removed and you now have the default System Policy on your computer.

5

Maintaining Packet Protect

You need to perform certain tasks to ensure that Packet Protect is running smoothly on their network.

In this chapter, you'll find information about:

- Monitoring Packet Protect computers.
- Setting Up Compatible Policies
- Installing a new adapter for a Packet Protect computer.
- Working with other security products.
- Turning security on.
- Turning security off.

Monitor Packet Protect Computers

View Status at a Packet Protect Client

At each computer, you can verify if Packet Protect is running.

To verify whether Packet Protect is running

1. At the taskbar on the computer, select Settings > Control Panel.
2. Double-click Services and verify that Intel Policy Agent is started.

If Intel Policy Agent doesn't appear in the list, Packet Protect has been shut down or is not functioning properly. See "Turn Security on Manually for an Existing Computer" on page 47 for details about restarting Packet Protect.

Set Up Compatible Policies

Two Packet Protect-enabled computers must agree on certain settings in order to communicate in a protected way. These settings must be agreed upon by both computers. It becomes increasingly difficult to set up an IPSec security system if there is a different network administrator who manages computers with which you need to communicate using Packet Protect.

Contact the other network administrator who is also using Packet Protect to coordinate the management of Packet Protect computers. One of you may need to update your client's System Policy to be compatible with the other computer's System Policy.

Two computers must use compatible settings for the following:

- **Authentication.** Both computers must use the same method to authenticate each other's identity (e.g., both computers must use the same pre-shared key)
- **IPSec.** Both computers must use compatible IPSec settings. See "Customize Security Actions" on page 33 and "How Packet Protect Uses IPSec" on page 59 for a list of the required settings.

Work with Other Security Products

On your network, there may be installations of an IPSec product other than Packet Protect. If this is the case, make sure that the security settings used by your computers match the security settings used by the other IPSec computers. This is because two IPSec-enabled computers must agree on these security settings in order to communicate in a protected way.

You might be managing both security product deployments, in which case you can verify the settings that need to match. If another network administrator manages the security computers using a different product, contact that network administrator to verify the settings.

Note: If the other network administrator manages Windows® 2000 IPSec computers, you will need to create a separate destination workgroup for each Windows 2000 IPSec computer. This will maximize IPSec interoperability.

In order to communicate with a Packet Protect computer using IPSec, the two computers must use compatible settings for the following:

- **Authentication.** Both computers must use pre-shared keys (the pre-shared key must be the same for both computers) to authenticate each other's identity.
- **IKE.** Both computers must use compatible IKE settings. See "How Packet Protect Uses IKE" on page 55 for a list of settings.
- **IPSec.** Both computers must use compatible IPSec settings. See "Customize Security Actions" on page 33 and "How Packet Protect Uses IPSec" on page 59 for a list of the required settings.

Note: If you decide to install Packet Protect for a computer that currently uses a different IPSec product, uninstall the other product, then install Packet Protect. For more information about installation, see "Install Security for a New Computer" on page 47.

Turn Security On for a Computer

After general deployment of Packet Protect, you might need to turn security on for a computer if the computer is new and hasn't had Packet Protect installed before. Or, you might need to manually turn Packet Protect on for an existing computer if Packet Protect was turned off previously.

Install Security for a New Computer

If a new computer requires Packet Protect, follow the instructions under "Install Packet Protect" on page 17.

Turn Security on Manually for an Existing Computer

After installation, Packet Protect is designed to start automatically upon system startup. If for some reason Packet Protect isn't running, you can restart it.

If you turned off security for a client and are now turning it back on, make sure you reverse whatever method you used to turn it off. See "Turn Security Off for a Computer" on page 48 for details about the ways you can turn off Packet Protect at a client.

To manually turn Packet Protect on

1. At the taskbar on the computer, select Settings > Control Panel.
2. Double-click Services.
3. Select Intel Policy Agent and click Start.

Turn Security Off for a Computer

There may be cases when you need to remove security from a client. For example, when the computer no longer requires protected traffic. There are two ways you can remove security from a client:

1. Shut down Packet Protect at the computer
2. Uninstall Packet Protect at the computer

Shut Down Packet Protect at a Computer

Packet Protect is designed to run automatically every time the computer starts. You can shut down Packet Protect for the current session, or you can change the computer setup so Packet Protect doesn't run each time the computer starts.

To shut down Packet Protect for the current computer session

1. At the taskbar on the computer, select Settings > Control Panel.
2. Double-click Services.
3. Select Intel Policy Agent and click Stop.

Note: If you want to turn security on later, manually restart Packet Protect. See "Turn Security on Manually for an Existing Computer" for more information.

Uninstall Packet Protect from a Computer

Uninstalling Packet Protect from a computer permanently removes all Packet Protect-related files, including IPSec, IKE, policies, and related Packet Protect program files.

To uninstall Packet Protect

1. At the taskbar on the computer, select Settings > Control Panel.
2. Double-click Add/Remove Programs.
3. On the Install/Uninstall tab, Select Packet Protect and click Add/Remove. Follow the prompts to uninstall Packet Protect.

Caution: When you uninstall Packet Protect, you lose all your customizations.

6

Troubleshooting and FAQs

This chapter details tips for troubleshooting Packet Protect. This chapter also provides a list of frequently asked questions about the product.

Troubleshooting

Communication fails

If a Packet Protect computer cannot communicate with another computer, check the following:

- Verify that each computer's basic security settings are set to allow communication. If the computers are using advanced security settings, verify that the computers have matching rules. The rules must allow for a match between ESP and AH settings for the security action.
- If using pre-shared keys, verify that each computer is set up to use the same pre-shared key when communicating with each another. Note that pre-shared keys are case-sensitive.
- At the client, verify that Packet Protect is running. Click the Start button on the taskbar, select Settings > Control Panel. Double-click Services and verify that Intel Policy Agent is started.

Communication fails when passing through a firewall

Depending on the type of firewall, IPSec may affect the deployment in different ways:

- Some firewalls block outside-in traffic without performing network address translation (NAT). These firewalls can sometimes be configured to allow IPSec traffic to flow from within the network.
- Proxying firewalls use HTTP, Telnet, FTP and other application proxies or SOCKS to forward traffic. With these firewalls, IPSec cannot be used to protect traffic end-to-end. IPSec can be used within the local LAN, but all outside traffic will remain unprotected.
- If a gateway or firewall is present doing network address translation, IPSec cannot be applied since IPSec packets are encrypted and integrity-protected, making address and port substitution impossible.

The effects of IPSec on firewall policies vary greatly on the type and goals of the firewalls. Refer to your firewall vendor for information on IPSec support.

Packet Protect doesn't start automatically upon startup

At the computer, make sure that Packet Protect is started as a service. See "Turn Security On for a Computer" on page 47.

Multicast, Broadcast, and IGMP traffic isn't protected

Multicast traffic is always unprotected when you use Packet Protect because of IPSec standards. In addition, IGMP traffic is unprotected.

I changed the IP address or DNS name of a computer, now it can't communicate on the network

If you have custom rules, there may be other computers in the network that have an old IP address or DNS name of a computer in their rules. These rules must be modified to reflect the IP address/DNS name change.

I think some transmitted information is unprotected and it shouldn't be

- Check the security action settings of both computers to make sure they match. Also try to determine which rule is being applied to the communication. If the rule is set to allow the communication if the rule fails, the computers will transmit data “in the clear” (without security).
- Check the default behavior. If both computers use Secure Responder or No Security, they will always communicate in the clear. If none of the rules applies to the communication, the communication is unprotected if the default behavior is Secure Initiator or Secure Responder.
- When a computer begins communication with another computer, the first few seconds are allowed in the clear if the rule being used as a fallback clear setting or if there are no matching rules and the behavior is Secure Initiator or Secure Responder.
- The following ports always allow traffic to pass in the clear:
 - UDP port 53 (for DNS traffic)
 - UDP port 68 to UDP port 67 (for DHCP)
 - UDP port 137 to UDP port 137 (NetBIOS name service)
 - UDP port 138 to UDP port 138 (NetBIOS datagram service)
 - TCP any port to TCP port 389 (LDAP directory access)

Frequently Asked Questions (FAQs)

What is Packet Protect?

Packet Protect helps protect Internet Protocol (IP) traffic as it travels between computers on your LAN.

What is IPSec?

Internet Protocol (IP) Security is a set of protocols used to help secure the exchange of IP data. For more information about IPSec, see “*Appendix A — IKE and IPSec*” on page 53.

What is IKE?

Internet Key Exchange is a protocol used to verify the identity of computers and negotiate a protected communication. For more information about IKE, see “*Appendix A — IKE and IPSec*”.

How does Packet Protect work with multiple adapters?

Packet Protect can work with multiple adapters that you install in one computer. If you use an Intel® PRO/100 S Management or Server adapter, Packet Protect offloads encryption tasks to any of these adapters. For more information, see “Multiple Adapters” on page 16.

How does Packet Protect work with Adapter Teaming?

Adapter Teaming and Packet Protect work together only for computers with Windows NT* operating systems installed. For more information, see “Adapter Teaming” on page 16.

How does implementing Packet Protect affect my network performance?

Like any IPSec solution, Packet Protect decreases network performance because of the intense computation required to encrypt, decrypt, and validate packets. Use Packet Protect with an Intel PRO/100 S Management or Server Adapter to reduce the impact on processor utilization and network traffic. Packet Protect is designed to offload processor-intensive tasks (ESP and AH algorithm calculations) to these Intel adapters that are installed in a computer. This frees up the computer's processor utilization for other tasks, reducing the impact to the network performance.

How can I tell if Packet Protect is running?

From the Start menu, select Settings > Control Panel. Double-click Services and verify that Intel Policy Agent is started.

Why isn't Multicast, Broadcast, and IGMP traffic protected

Multicast traffic is always unprotected when you use Packet Protect because of IPSec standards. In addition, IGMP traffic is unprotected.

A

Appendix A — IKE and IPSec

A protected communication using Packet Protect involves Internet Key Exchange (IKE) and Internet Protocol Security (IPSec). This appendix describes details about IKE and IPSec, and how the technologies work together to protect information as it travels on your network.

In this appendix, you'll find the following information:

- An overview of IKE and IPSec.
- How Packet Protect uses IKE.
- How Packet Protect uses IPSec.

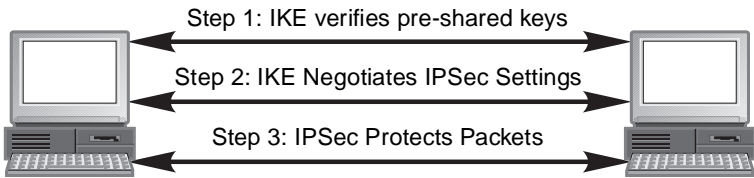
For more information about IKE and IPSec, including applicable RFCs, see Internet Engineering Task Force IPSec Working Group Web site at <http://www.ietf.org>.

IKE and IPsec Work Together

Packet Protect uses IKE and IPsec to protect packets traveling on the network:

- **IKE** — Negotiates the security settings to be used by IPsec for protection of the communication.
- **IPsec** — Protects the packets traveling between two computers that are attempting to communicate.

The following diagram illustrates how Packet Protect uses IKE and IPsec together to protect a communication between two computers.



How Packet Protect Uses IKE

IKE is a set of standard protocols developed by the Internet Engineering Task Force (IETF). IKE is used to authenticate and negotiate a protected communication. Using IKE is a two step process:

- 1 IKE verifies the pre-shared keys of the two computers that are attempting to communicate.
- 2 IKE negotiates a set of security settings to be used by IPSec.

Each computer must agree upon the security settings before IKE can establish a protected communication for IPSec.

Identity Negotiation Settings

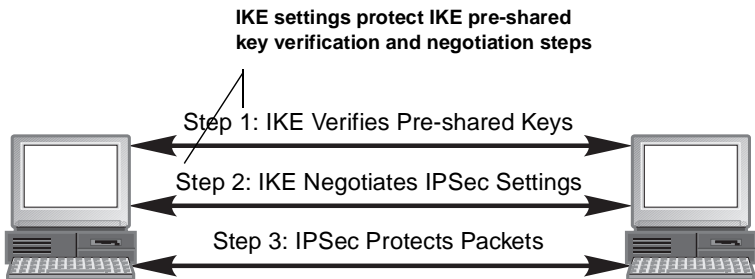
When IKE negotiates security for two computers, it requires that the following be compatible:

- IKE settings
- Authentication method

IKE Settings

IKE settings are agreed upon by the two computers that are attempting to verify each other's pre-shared key. They are used to protect the IKE negotiation transactions. This allows the two computers to negotiate without compromising secret key or password information.

The diagram below shows the steps that Packet Protect performs to protect a communication. The IKE settings are used during Steps 1 and 2.



Packet Protect uses pre-defined IKE settings, designed for maximum compatibility with computers that use Packet Protect and other IPSec products.

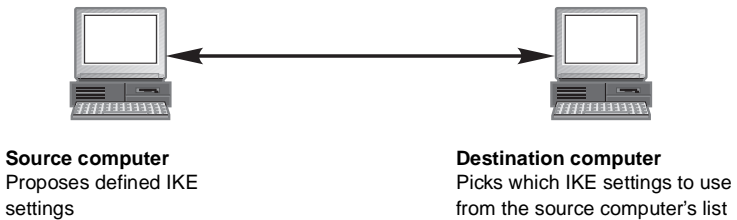
If two Packet Protect computers attempt to communicate, they use the same default IKE settings. If one of the computers is managed by a different IPSec product, make sure that the IKE settings match. If necessary, make changes to

the IKE settings in the other IPSec product. The following table describes the pre-defined IKE settings for each computer that uses Packet Protect.

Table 7: Pre-Defined IKE Settings

Preferred Order	Encryption	Hashing	Diffie-Hellman
1	DES (56-bit)	MD5	768-Bit
2	DES (56-bit)	SHA-1	768-Bit
3	3DES (168-bit) <i>Domestic version only</i>	MD5	1024-Bit
4	3DES (168-bit) <i>Domestic version only</i>	SHA-1	1024-Bit

A computer that requests a protected communication proposes its list of IKE settings to the computer with which it is trying to communicate. The IKE settings are proposed in order of preference, but the responding computer can agree on any of the proposed combinations. The responding computer must have one of the combinations defined, or the communication is not allowed using IPSec.



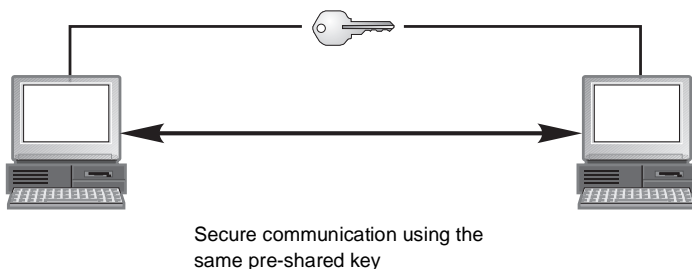
NOTE: The IKE settings used by Packet Protect cannot be customized. If you require different settings for a communication with a computer that uses a different IPSec product, change the IKE settings in the other product to match one of the IKE setting combinations used by Packet Protect (as noted in the above table).

Authentication Method

IKE requires that two computers use the same authentication method to verify each other's identity. Packet Protect supports the following:

- **Pre-shared keys** — If using pre-shared keys, the two computers attempting to communicate must propose the *same* pre-shared key, otherwise they cannot communicate using IPSec. If you change the pre-shared key for a workgroup, remember that this changes the pre-shared key used for all

communications for all computers in the workgroup.



IPSec Settings

After IKE verifies the identity of each computer, it negotiates which IPSec settings to use to protect the communication after negotiation. Packet Protect comes with pre-defined IPSec options, or you can create your own.

Each computer must agree upon the IPSec settings to use before IKE can establish a protected communication for data transfer.

Pre-defined IPSec Settings

Packet Protect comes with pre-defined IPSec settings, called security actions. These security actions are designed for maximum compatibility between computers using Packet Protect and other IPSec products.

A computer that requests a protected communication proposes its IPSec settings to the computer with which it is trying to communicate. The IPSec settings include a list of algorithm combinations that appear in order of preference. The other computer must allow one of these defined algorithm combinations, otherwise, the communication is not allowed using IPSec.

For a description of the individual IPSec settings and how you might use them, see “Available Settings for Security Actions” on page 34.

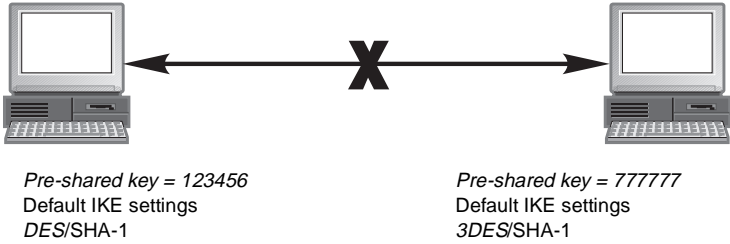
Custom IPSec Settings

Although it is recommended that you use the pre-defined IPSec settings (security actions) that come with Packet Protect, you can also create your own to meet your custom corporate security guidelines. If you create your own, keep in mind that two computers must agree on certain settings in order to communicate using IPSec.

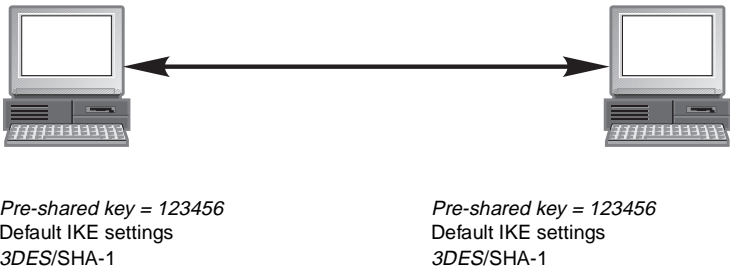
For more information about creating your own IPSec security actions, see “Customize Security Actions” on page 33.

Examples

The following diagram illustrates failed IKE negotiations due to *mismatched* settings.



The following diagram illustrates successful IKE negotiations due to *matched* settings.



How Packet Protect Uses IPSec

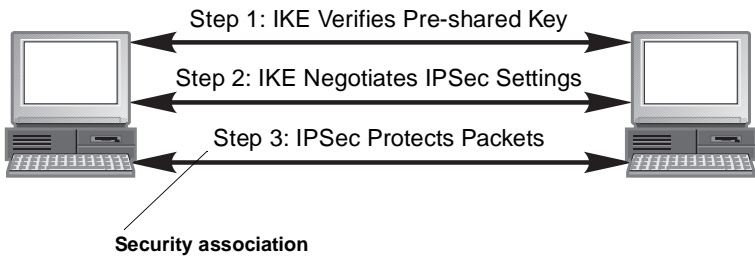
IPSec is a set of standard protocols developed by the Internet Engineering Task Force (IETF). IPSec is used to protect the privacy and integrity of IP communications. It protects IP communications using algorithms that perform encryption and authentication tasks, as well as other features that enforce additional protection.

If IKE successfully negotiates a protected communication, it passes the agreed upon information to the IPSec driver used by Packet Protect. Then, the IPSec driver uses that information to determine how to protect the IP communication.

Security Associations

IP communications use a security contract or *security association* when they are protected using IPSec. After a security association is set up between two computers, the computers can exchange data and IPSec will protect that data using one or more of ESP encryption, ESP authentication, or AH authentication algorithms.

The diagram below shows the steps that Packet Protect performs to protect a communication. The security association is established in Step 3.



For more information about each IPSec setting, see “IPSec Settings” on page 57 and “Customize Security Actions” on page 33.

Security Association Lifetimes

Security associations expire if they reach the maximum threshold defined for the communication. Packet Protect is designed to automatically re-negotiate the security association when it is about to expire (usually when it reaches approximately 80% of its lifetime), if one of the following is true:

- The security action is currently in use, that is, data is being transferred currently.
- The security action has been used recently, that is, data was transferred using that security association.

Packet Protect re-negotiates the IPSec settings only; it doesn't need to re-verify the identity of the computers because it is already known. This helps reduce network traffic by reducing extra key generation.

If the security association is not renewed automatically and consequently expires, a security association between the same computers will require both IKE steps: pre-shared key verification and IPSec negotiation.

How IPSec Protects Packets

IPSec applies the selected algorithms to each packet that is protected by IPSec. The algorithms provide one of the following protection features:

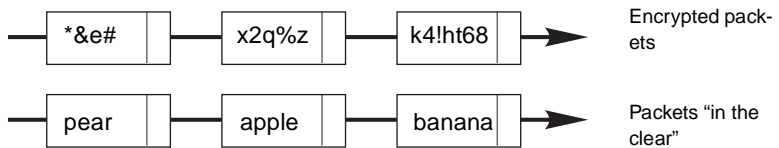
- Encryption and privacy
- Integrity
- Time and size limits
- Anti-replay protection

The following sections describe some technical detail about encryption and integrity protection. The other features of IPSec are described in "Customize Security Actions" on page 33.

Encryption

Use encryption to protect the confidentiality of packets. Encryption encodes packets so they are unreadable unless the receiver has the proper key to decode the packets.

If a packet is encrypted using ESP encryption (DES or 3DES algorithms), it is unreadable while in transit. Other types of encryption can protect the confidentiality of information while stored on a computer – Packet Protect is designed to protect the confidentiality of information while traveling on the network. The following diagram shows unencrypted and encrypted packets traveling on the network.



If the packets pass through any routers or switches, the encrypted packets are relayed without requiring IPSec on those devices.

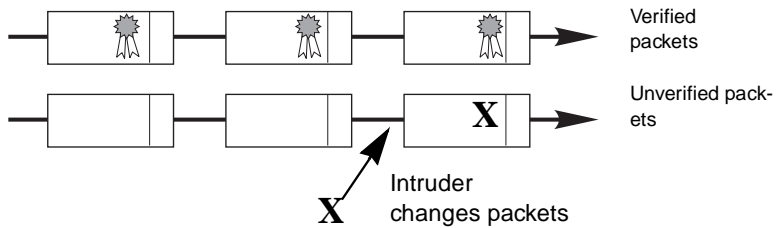
Integrity

Data integrity verifies that the packet was unchanged during transport over the network. It also verifies that other packets were not inserted into the packet flow. This helps prevent a computer from accepting packets from an intruder who is attempting to send packets on the network.

Use integrity features to protect the authenticity of packets, that is, verify that the packet was unchanged during transport over the network. Integrity features also verify that no other packets were inserted into the packet flow.

Packet Protect uses ESP and AH algorithms (MD5 or SHA-1) to protect the integrity of packets.

The following diagram shows two sets of packets traveling on the network. The first set uses integrity protection; the second set does not.



B

Appendix B — Interoperability with Microsoft Windows* 2000

An overview of interoperability between Windows 2000 computers and Packet Protect computers.

Interoperability with Windows* 2000

By default, IPSec is not enabled in Windows 2000. Windows 2000 is installed with “No Security” as the IPSec default action. You can use the IP Security Policy Management tool to activate IPSec in Windows 2000.

Windows 2000 has three IPSec default behaviors—Server, Secure Server, and Client—that you can choose from when you configure the computer.

Currently, Packet Protect interoperates with Windows 2000 using a pre-shared key. However, because Windows 2000 default authentication mechanism is Kerberos, which is not supported by Packet Protect, the authentication must be changed to use pre-shared keys. Be sure to use the same pre-shared keys on Windows 2000 computers as Packet Protect-enabled computers for proper interoperability.

Tips: If you have Windows 2000 computers and want them to communicate securely with Packet Protect-enabled computers, you must use the Default Rule that is set up with the Packet Protect System Policy. Do not erase or modify the Default Rule for best results.

For maximum interoperability, be sure to place each Windows 2000 computers in its own Destination Workgroup.

Creating Policies

To create custom IPSec policies in Windows 2000

1. On the taskbar, click Start and select Settings > Control Panel.
2. Double-click Network and Dial-up Connections.
3. Right-click Local Area Connection and select Properties.
4. Click Advanced and select the Options tab.
5. Under Optional settings, click IP security.
6. Click Properties.
7. Click Use this IP security policy, and then select the IPSec policy you want to use.

You can also use the IP Security Policies snap-in in the Microsoft Management Console (MMC). Set it to use the local computer, right-click the policy you want to use, and then click Assign.

You must be a member of the Administrators group to set IPSec policies. If a computer participates in a Windows 2000 domain, the computer may receive the IPSec policy from Active Directory, overriding the local IPSec policy. In this case, the options are disabled and you cannot change them from the local computer.

C

Appendix C — Network Software License Agreement

This appendix details the following:

- Network Software License Agreement
- Intel Automated Customer Support

Network Software License Agreement

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software and any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE. You may copy the Software onto a single computer for your personal, non-commercial use, and you may make one back-up copy of the Software, subject to these conditions:

1. **This Software is licensed for use only in conjunction with Intel component products. Use of the Software in conjunction with non-Intel component products is not licensed hereunder.**
2. You may not copy, modify, rent, sell, distribute or transfer any part of the Software except as provided in this Agreement, and you agree to prevent unauthorized copying of the Software.
3. You may not reverse engineer, decompile, or disassemble the Software.
4. You may not sublicense or permit simultaneous use of the Software by more than one user.
5. The Software may contain the software or other property of third party suppliers, some of which may be identified in, and licensed in accordance with, any enclosed "license.txt" file or other text or file.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the Software, or to items referenced therein, at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY. If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

LIMITATION OF LIABILITY. IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

TERMINATION OF THIS AGREEMENT. Intel may terminate this Agreement at any time if you violate its terms. Upon termination, you will immediately destroy the Software or return all copies of the Software to Intel.

Intel Automated Customer Support

You can reach Intel's automated support services 24 hours a day, every day at no charge. The services contain the most up-to-date information about Intel products. You can access installation instructions, troubleshooting information, and general product information.

Readme Files on Your Product Disk

To review the readme topics, insert the PRO/100 S Server or Management adapter disk in a disk drive, switch to that drive, and type:

`SETUP /README` and then press Enter.

Web and Internet Sites

Support: <http://support.intel.com>

Network Products: <http://www.intel.com/network>

Corporate: <http://www.intel.com>

FTP Host: download.intel.com

FTP Directory: [/support/network/adapter/](http://support/network/adapter/)

Customer Support Technicians

US and Canada: 1-916-377-7000 (7:00 - 17:00 M-F Pacific Time)

Worldwide access: Intel has technical support centers worldwide. Many of the centers are staffed by technicians who speak the local languages. For a list of all Intel support centers, the telephone numbers, and the times they are open, go to:

<http://support.intel.com/support/9089.htm>.

G

Glossary

3DES

Triple Data Encryption Standard, or Triple DES. An encryption standard used to encode data while it travels on a network. 3DES uses 168-bit keys to encrypt data.

3DES is available only in the domestic version of Packet Protect.

AH

Authentication Header. A protocol of verifying the integrity of packets, that is, the packets are known to be from the originating computer. Packet Protect uses MD5 and SHA-1 to authenticate packets.

anti-replay

Protection against receiving repeat data transmitted on the network. This helps prevent an intruder from successfully sending the same data in an attempt to confuse the system (for example, the computer could repeat the task of restarting a server).

authentication

The process of verifying the identity of a computer. Packet Protect authenticates a computer using pre-shared keys. It helps verify that a computer is who it claims to be.

cryptography

The science of protecting the privacy of data by encoding the data so it is unreadable to anyone who doesn't have a secret key to decode it.

CPU utilization

A measurement of the average load on a computer's processor. As processor usage increases due to security tasks, users may notice slower performance. Intel PRO/100 S Management and Server Adapters are designed to offload the security overhead from Packet Protect by using a special on-board processor, thereby reducing processor utilization.

decryption

The un-encoding of encrypted data using a secret password or key.

DES

Data Encryption Standard. An encryption standard used to protect data confidentiality by encoding the data before it travels on a network. Packet Protect supports 56-bit DES and 168-bit 3DES (3DES available in the United States and Canada only).

destination workgroup

A logical collection of computers (servers and clients) that you define in Packet Protect. Destination workgroups contain lists of computers with which a computer in the source workgroup may want to communicate using IPsec.

Destination workgroups in Packet Protect are different from workgroups in Windows operating systems.

default behavior

The setting for a workgroup specified in Packet Protect that determines how a computer communicates using IPsec.

Diffie-Hellman

A method of sharing a secret key between two computers.

DNS

Domain Name Server. The network of Domain Name Servers that resolve fully qualified domain names (FQDNs) to their corresponding IP addresses.

encryption

The process of protecting data confidentiality by encoding the data so it is unreadable to anyone who doesn't have the secret key to decode it. You can read data if it isn't encrypted, but you can't read data while it's encrypted.

ESP

Encapsulation Security Payload. A method of protecting the confidentiality and/or integrity of data. ESP can be used

to protect data confidentiality by encrypting the data using DES or 3DES. ESP can also be used to verify the origination of data by authenticating the data using MD5 or SHA-1.

FQDN

Fully Qualified Domain Name. The unique name given to a computer or device. When addressing information or requests, it's often easier to remember a fully qualified domain name rather than an IP address. Because computers communicate using IP addresses, DNS software matches the fully qualified domain name to its corresponding IP address so users can communicate using the domain name and the IP address.

ICMP

Internet Control Message Protocol. A type of IP protocol used to transmit data that typically contains error or explanatory information. For example, the ping command uses ICMP to transmit data about network connectivity.

IETF

Internet Engineering Task Force. The organization that is developing and standardizing IKE and IPsec.

IKE

Internet Key Exchange. A protocol built on standards that is used to negotiate a protected communication.

IKE is a subset profile of ISAKMP/Oakley. It is being developed by the Internet Engineering Task Force (IETF).

intruder

An unwanted visitor from inside or outside your company who may try to steal information or harm your network.

IP

Internet Protocol. A set of rules that

describe how computers transmit data with a destination address.

IP address

A series of numbers that identifies a connection point or device on an IP network. Each connection point and device needs a unique IP address to communicate using IP. For example, 192.168.1.1 is a sample IP address.

IPSec

Internet Protocol (IP) Security. A set of protocols used to help secure the exchange of IP data. IPSec is being developed by the Internet Engineering Task Force (IETF).

key

A set of bytes that encrypt or decrypt data. Keys allow you to protect data from being read by an intruder on the network. Keys can be symmetric or asymmetric and asymmetric keys can be either public or private.

LAN

Local Area Network. A communications network usually located within a building or small number of buildings. For example, computers and printers at many companies are connected to a LAN.

lockdown

A description of a default behavior for a computer that uses Packet Protect. A Lockdown computer initiates and replies to all communications by requesting security; it only communicates using IPSec (requires that the other computer also uses IPSec). A common use for this setting is a server that requires very restricted access.

MD5

Message Digest Algorithm. An algorithm often used to verify the integrity of packets traveling on a network. The algorithm transforms any number of bytes into a

fixed number of bytes; no other set of bytes produces the same result.

network

One or more computers that are connected together for communication purposes.

offload

The assignment of algorithm computations from software to hardware. Packet Protect offloads security tasks to Intel PRO/100 S Management and Server adapters to speed processing and increase network performance.

packet

A piece of data that travels on the network. Each packet contains the data being transmitted, along with a destination address. Packet Protect protects packets as they travel on the network using IPSec.

perfect forward secrecy

The generation of an additional key pair to be used during data transfer. This helps guarantee that no keys are re-used. Using perfect forward secrecy increases protection, but generates more CPU utilization.

policy

A collection of security settings and rules that are applied to a group of computers.

port

A connection point used by IP applications. For example, a Web server typically sends and receives information on port 80.

pre-shared key

A secret password that a computer presents to help verify its identity. Pre-shared keys are used during negotiation of a secure communication. Each computer must present the same pre-shared key in order to communicate using IPSec.

protocol

A set of guidelines that describe how net-

works or applications communicate. If the set of rules are followed, information can be processed correctly. This allows computers and hardware devices to communicate with one another even if they're different from one another.

rule

A definition of the security settings to apply when a computer communicates with a destination computer using a specified protocol.

secure initiator

A description of a default behavior for a computer that uses Packet Protect. A Secure Initiator computer initiates communications by requesting security and responds to communication requests without security ("in the clear"). A common use for this setting is a server that doesn't require the strict control of the Lockdown setting.

secure responder

A description of a default behavior for a computer that uses Packet Protect. A Secure Responder computer initiates communications without security ("in the clear"), but can respond to communication requests with security. A common use for this setting is a workstation.

security action

A collection of IPSec settings that are proposed when two computers attempt to communicate. Packet Protect uses security actions when a rule is matched for a communication.

security association

A security contract between two computers. While the security association is active (8 hours is the default), the two computers can send data without re-negotiating a communication (as long as the data being sent uses a protocol defined in

the existing security association).

security association lifetime

The duration of a security association. A lifetime can be limited by time or by the amount of data transmitted.

SHA-1

Secure Hash Algorithm. An algorithm often used to verify the integrity of packets traveling on a network. The algorithm transforms any number of bytes into a fixed number of bytes.

traffic

Packets traveling on the network.

workgroup

A logical collection of computers (servers and clients) that you define in Packet Protect.

Workgroups in Packet Protect are different from workgroups in Windows operating systems.

Index

A

adapters

- installing 15
- teaming and 16
- use multiple 16

algorithms and security actions 35

Anti-replay protection 4

anti-replay protection 35

authentication

- of rules 26

C

clients

- failed communication between 50
- turn off security for 48
- turn on security for 47
- uninstalling Packet Protect from 48

configure adapters for Packet Protect 15

customize

- destination workgroups 31

D

Data Encryption Standard 60

data integrity 60

DES. See Data Encryption Standard

destination workgroups

- customize 31
- modify 33
- modify after policy distribution 41

domestic version of Packet Protect 2

E

Encapsulation Security Payload 60

encryption algorithms 35

encryption of data packets 4, 60

ESP. See Encapsulation Security Payload

export version of Packet Protect 2

F

FAQs. See Frequently Asked Questions

firewall

- using Packet Protect with 50

firewalls 50

Frequently Asked Questions 49

G

gateway 50

glossary 69

H

hardware

- acceleration 2

hardware acceleration 2

help file for Packet Protect 3

I

IKE. See Internet Key Exchange

installation

- more information ii

- notes ii

integrity of data packets 4

Internet Key Exchange

- authentication 56

- definition 4

- how it works with IPSec 54

- how Packet Protect uses 55

- settings 55

Internet Protocol Security

- data integrity and 60

- definition 4

- encryption of data packets 60

- how it protects packets 59, 60

- how it works with IKE 54

- how Packet Protect uses 59

- security associations and 59

- settings 57

Internet Protocol traffic

- protection of 1

- traffic not protected by Packet Protect 50, 52

interoperability with other security products 46

introduction 1–6

intruders 1

IP. See Internet Protocol

IPSec. See Internet Protocol Security

L

LAN. See Local Area Network

Local Area Network 1

Lockdown workgroup behavior 23

N

network address translation 50

O

ordering rules 27

other security products

 interoperability with 43

overview 2

overview of Packet Protect 2

P

Packet Protect

 administrator and client versions 3

 domestic and export versions 2

 features 2

 frequently asked questions 49

 get started 6

 getting started 6

 how it works 4

 HTML help 3

 introduction 1

 preparing for installation 8

 purpose 2

 troubleshooting 49

 work with other IPSec products 46

perfect forward secrecy 35

policy

 definition of 25

 modifying after distribution 40

 set up compatible policies 45

R

readme files ii

rules

 authentication setting 26

 definition of 25

 delete after policy distribution 41

 If rule fails 26

 importance of order 25, 27

 ordering 31

S

Secure Initiator workgroup behavior 23

Secure Responder workgroup behavior 22

security action

 customize 33

security actions

- create new 36

- customize 33

- definition of 26

- modify after policy distribution 41

services on the World Wide Web ii

size limit and security actions 34

support services 67

T

time limit and security actions 34

troubleshooting 49

- more information ii

U

uninstalling

- Packet Protect at clients 48

V

view

- status at clients 44

W

workgroups

- customize security actions 33

- modify destination workgroups 31